Azure Identity and Access Management tasks

author:Dibrova Volodymyr

Practical Task 1: Introduction to Microsoft Entra ID

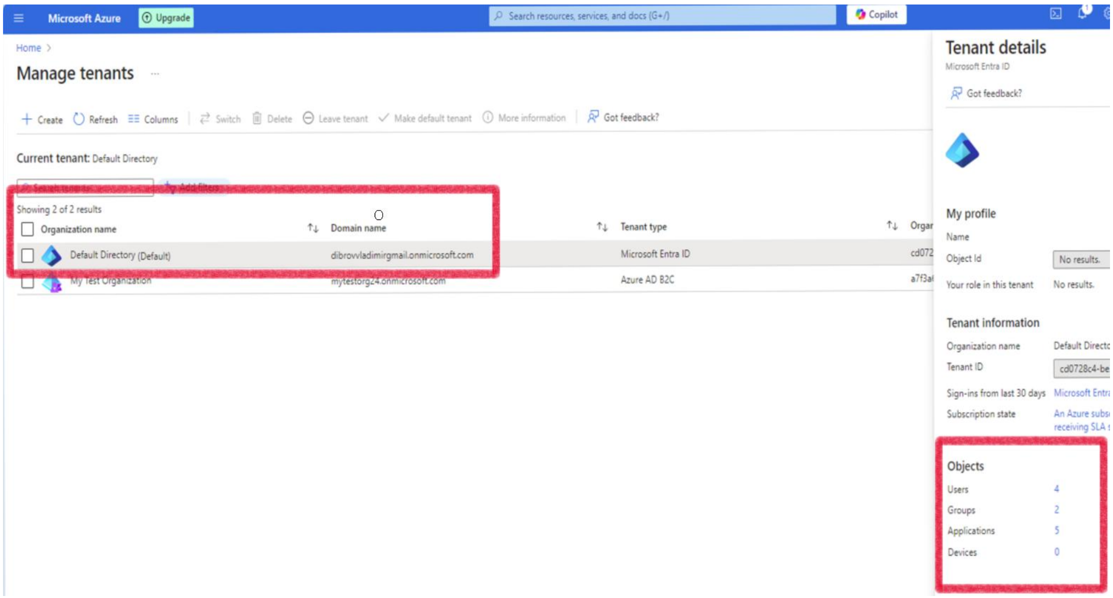
Create a basic Microsoft Entra ID setup for an organization to manage identity and access.

Requirements:

1. Create a new Microsoft Entra ID tenant.
2.
2. Add at least two users to the directory.
3. Create two groups named **Developers** and **Admins**.
4. Assign the users to appropriate groups.
5. Assign the **Global Reader** role to the **Admins** group.
6. Assign the **Application Developer** role to the **Developers** group.
7. Verify that the role assignments function as expected for both groups.

Actions Taken:

- Used Default Microsoft Entra ID instead of creating a new tenant due to issues with phone number registration.



Manage tenants

Current tenant: Default Directory

Showing 2 of 2 results

Organization name	Domain name	Tenant type	Orgar
Default Directory (Default)	dibrovvladimirgmail.onmicrosoft.com	Microsoft Entra ID	cd072
My Test Organization	mytestorg24.onmicrosoft.com	Azure AD B2C	a7f3a

Tenant details

Microsoft Entra ID

My profile

Name

Object Id: No results.

Your role in this tenant: No results.

Tenant information

Organization name: Default Directo

Tenant ID: cd0728c4-be

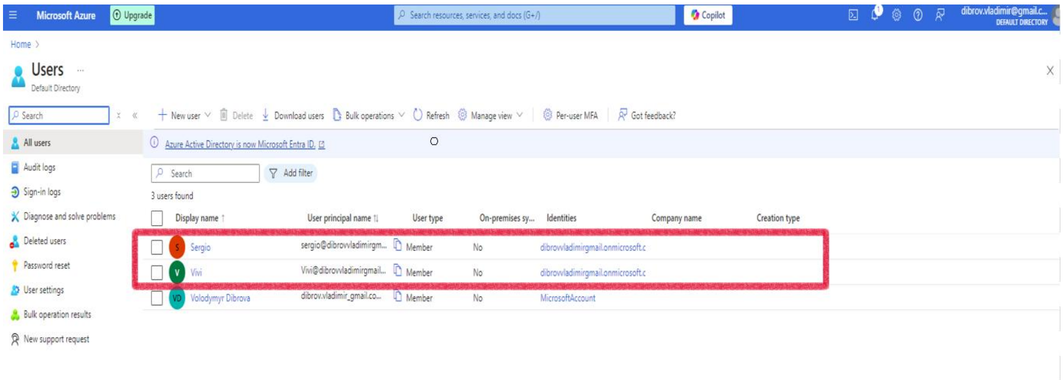
Sign-ins from last 30 days: Microsoft Entra

Subscription state: An Azure subs receiving SLA

Objects

Users	4
Groups	2
Applications	5
Devices	0

- Added two users

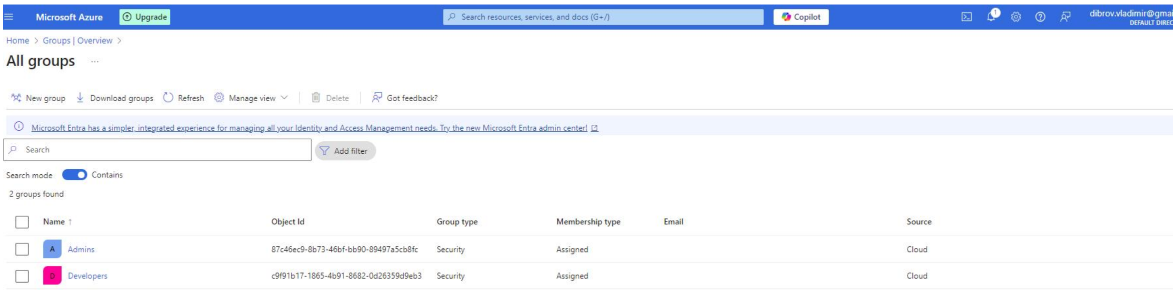


3 users found

Display name	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
Sergio	sergio@dibrovvladimirgm...	Member	No	dibrovvladimirgmail.onmicrosoft.c		
Vivi	Vivi@dibrovvladimirgmail...	Member	No	dibrovvladimirgmail.onmicrosoft.c		
Volodymyr Dibrova	dibrov.vladimir_gmail.co...	Member	No	MicrosoftAccount		

- Created two groups:

1. **Developers**
2. **Admins**

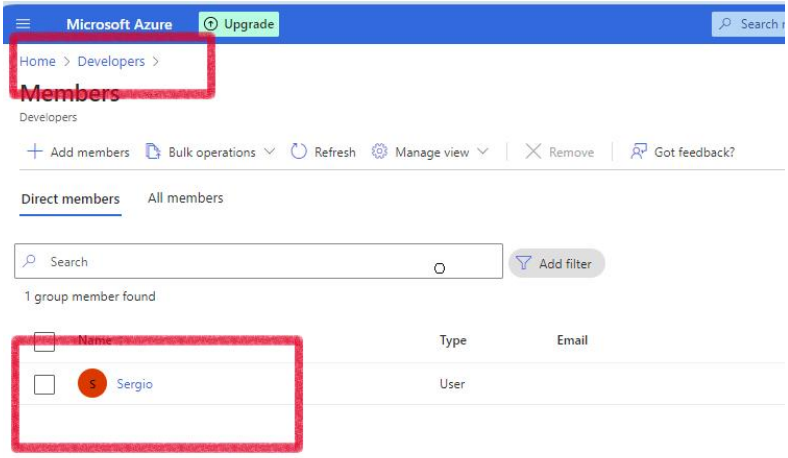

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
dibrov.vladimir@gmai
DEFAULT DIREC
Home
Groups | Overview
All groups
New group
Download groups
Refresh
Manage view
Delete
Got feedback?
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!
Search
Add filter
Search mode
Contains

2 groups found

Name	Object Id	Group type	Membership type	Email	Source
Admins	87c46ec9-8b73-46bf-bb90-89497a5cb8fc	Security	Assigned		Cloud
Developers	c9f91b17-1865-4b91-8682-0d26359d9eb3	Security	Assigned		Cloud

- Assigned users to the appropriate groups:

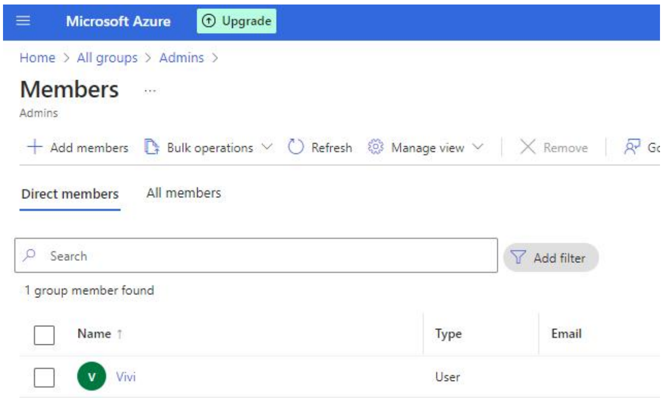
1. Developers: Sergio



1 group member found

Name	Type	Email
Sergio	User	

2. Admins: Vivi



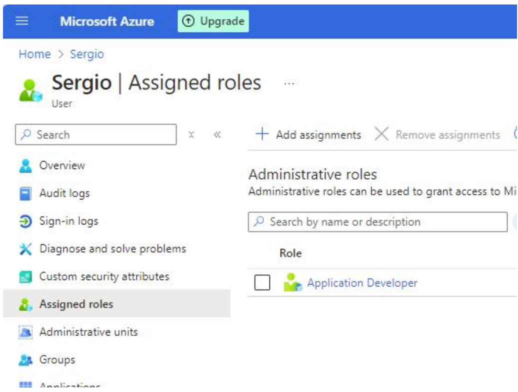
Members ···

Admins

1 group member found

□	Name ↑	Type	Email
□	V Vivi	User	

- Assigned roles:
- **The first version**



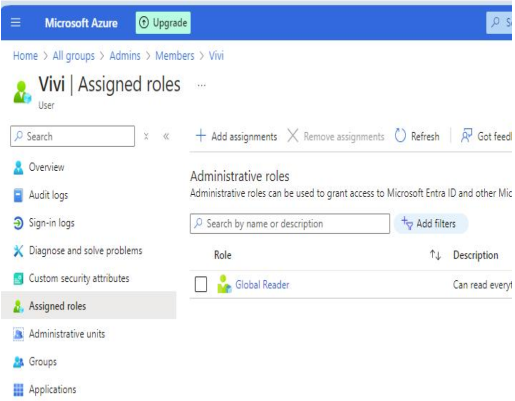
Sergio | Assigned roles ···

User

Administrative roles

Administrative roles can be used to grant access to Mi

□	Role
□	Application Developer



Vivi | Assigned roles ···

User

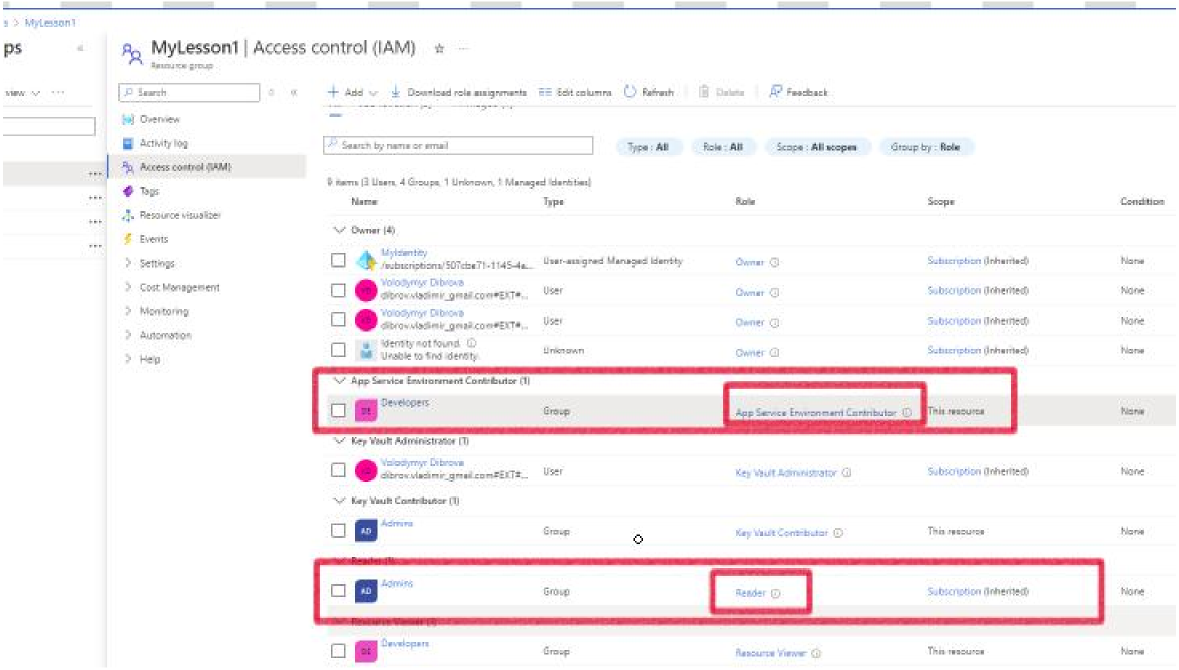
Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Mic

□	Role ↑↓	Description
□	Global Reader	Can read everyt

- **The second version:**

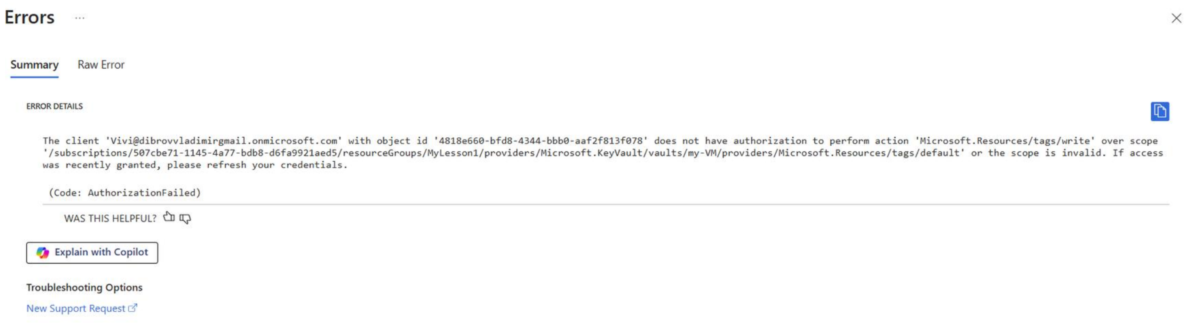
1. **Reader** role was assigned to the Admins group instead of the **Global Reader** role
2. **App Service Environment Contributor** role was assigned to the Developers group instead of the **Application Developer** role.



9 items (3 Users, 4 Groups, 1 Unknown, 1 Managed Identities)

Name	Type	Role	Scope	Condition
Owner (4)				
MyIdentity /subscriptions/507cbe71-1145-4a...	User-assigned Managed Identity	Owner	Subscription (Inherited)	None
Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Owner	Subscription (Inherited)	None
Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Owner	Subscription (Inherited)	None
Identity not found. Unable to find identity.	Unknown	Owner	Subscription (Inherited)	None
App Service Environment Contributor (1)				
Developers	Group	App Service Environment Contributor	This resource	None
Key Vault Administrator (1)				
Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Key Vault Administrator	Subscription (Inherited)	None
Key Vault Contributor (1)				
Admins	Group	Key Vault Contributor	This resource	None
Reader (1)				
Admins	Group	Reader	Subscription (Inherited)	None
Resource Viewer (1)				
Developers	Group	Resource Viewer	This resource	None

Verified test(Try to create a new resource by user Vivi)



ERROR DETAILS

```
The client 'Vivi@dibrovvladimirgmail.onmicrosoft.com' with object id '4818e660-bfd8-4344-bbb0-aaf2f813f078' does not have authorization to perform action 'Microsoft.Resources/tags/write' over scope
'/subscriptions/507cbe71-1145-4a77-bdb8-d6fa9921aed5/resourceGroups/MyLesson1/providers/Microsoft.KeyVault/vaults/my-VM/providers/Microsoft.Resources/tags/default' or the scope is invalid. If access
was recently granted, please refresh your credentials.

 (Code: AuthorizationFailed)
```

Implementation Highlights:

- Using Default Entra ID allowed bypassing registration restrictions and successfully completing the task.

Practical Task 2: Enabling Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

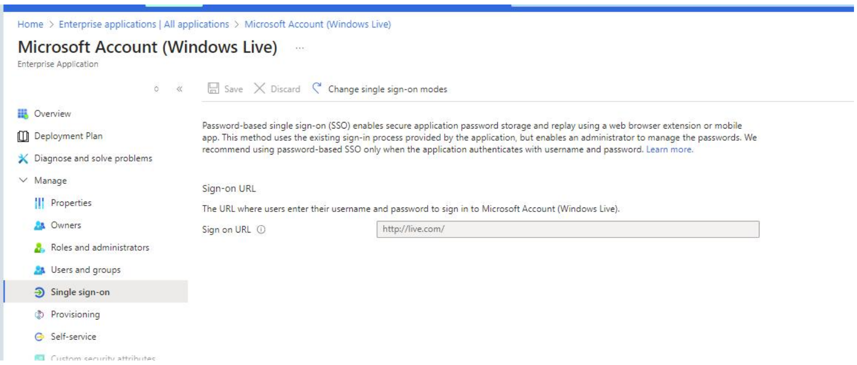
Configure Single Sign-On (SSO) and Multi-Factor Authentication (MFA) for users in a Microsoft Entra ID
directory to enhance identity and access security.

Requirements:

1. Enable Single Sign-On (SSO) for your Microsoft Entra ID tenant.
2. Enforce Multi-Factor Authentication (MFA) for all users in the directory.
3. Configure conditional access policies to require MFA for high-risk sign-ins.
4. Verify that SSO and MFA settings are correctly applied for the users.

Actions Taken:

1. **Single Sign-On (SSO)** by **Password-based** was successfully enabled for Microsoft Entra ID.


Home > Enterprise applications | All applications > Microsoft Account (Windows Live)
Save
Discard
Change single sign-on modes
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes

Microsoft Account (Windows Live) ···

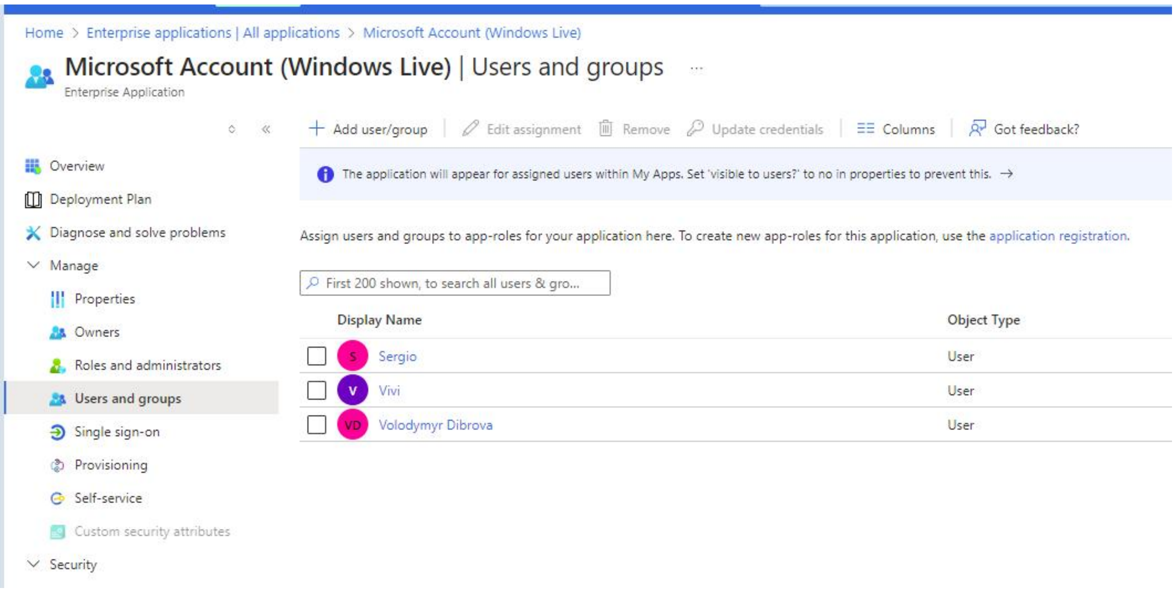
Enterprise Application

Password-based single sign-on (SSO) enables secure application password storage and replay using a web browser extension or mobile app. This method uses the existing sign-in process provided by the application, but enables an administrator to manage the passwords. We recommend using password-based SSO only when the application authenticates with username and password. Learn more.

Sign-on URL

The URL where users enter their username and password to sign in to Microsoft Account (Windows Live).

Sign on URL ⓘ http://live.com/



Microsoft Account (Windows Live) | Users and groups ···

Enterprise Application

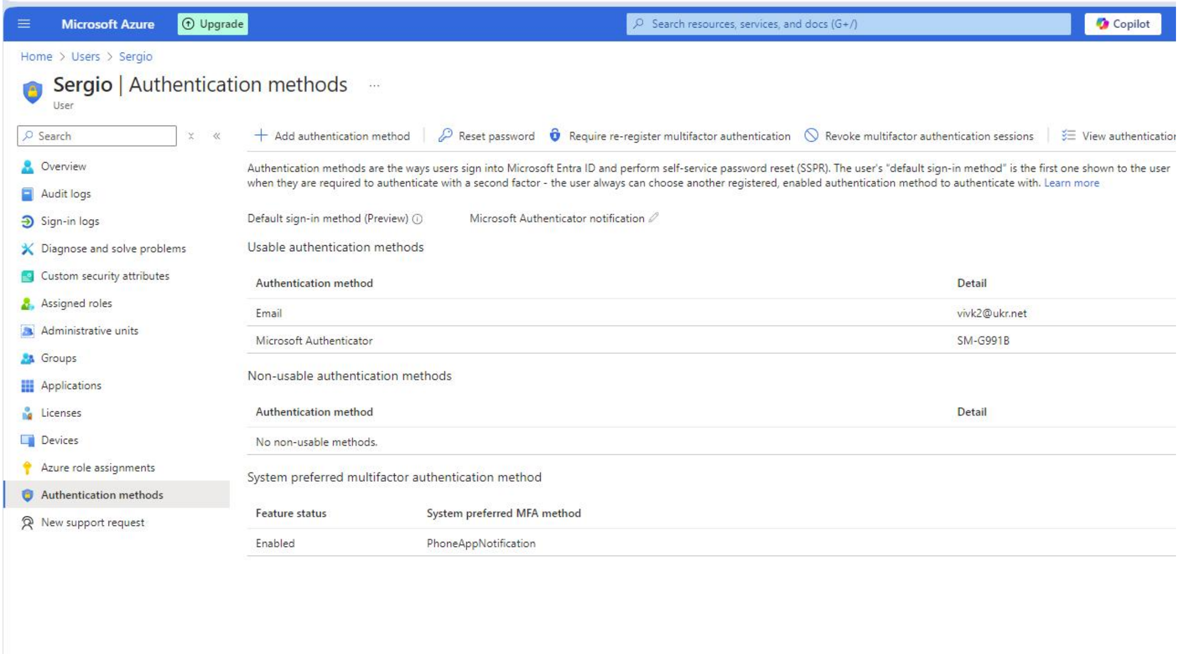
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.

First 200 shown, to search all users & gro...

	Display Name	Object Type
□	S Sergio	User
□	V Vivi	User
□	VD Volodymyr Dibrova	User

2. **Multi-Factor Authentication (MFA)** was activated for all users in the directory.



Sergio | Authentication methods

User

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
Email	vivk2@ukr.net
Microsoft Authenticator	SM-G991B

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	PhoneAppNotification

Configure conditional access policies to require MFA for high-risk sign-ins.

Due to registration limitations for a Premium P2 license (mobile phone number issue), the configuration was performed manually without Premium P2

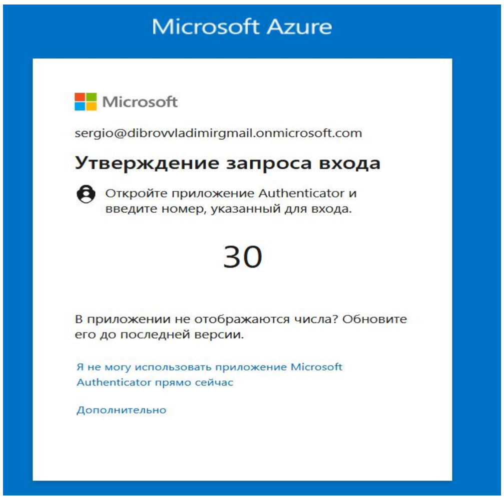
- Configured **MFA status as Enabled** for all users in the directory.
- Navigated to **Azure Active Directory > Security > Conditional Access > Named Locations** to define trusted IP addresses (currently unavailable).
- Ensured MFA is configured for each application individually to enhance security for high-risk sign-ins.
- Used **Subscriptions > Access Control (IAM) > Add Role Assignment** to assign roles requiring MFA for the necessary resources.

Results:

- Achieved a manual setup approximating **high-risk sign-in** scenarios through customized configurations.
- Secured access with **SSO and MFA** functioning effectively.

3. Verification completed:

    1. SSO and MFA are functioning as expected, enhancing access security.



Microsoft Azure

Microsoft

sergio@dibrovvladimirgmail.onmicrosoft.com

Утверждение запроса входа

Откройте приложение Authenticator и введите номер, указанный для входа.

30

В приложении не отображаются числа? Обновите его до последней версии.

Я не могу использовать приложение Microsoft Authenticator прямо сейчас

Дополнительно

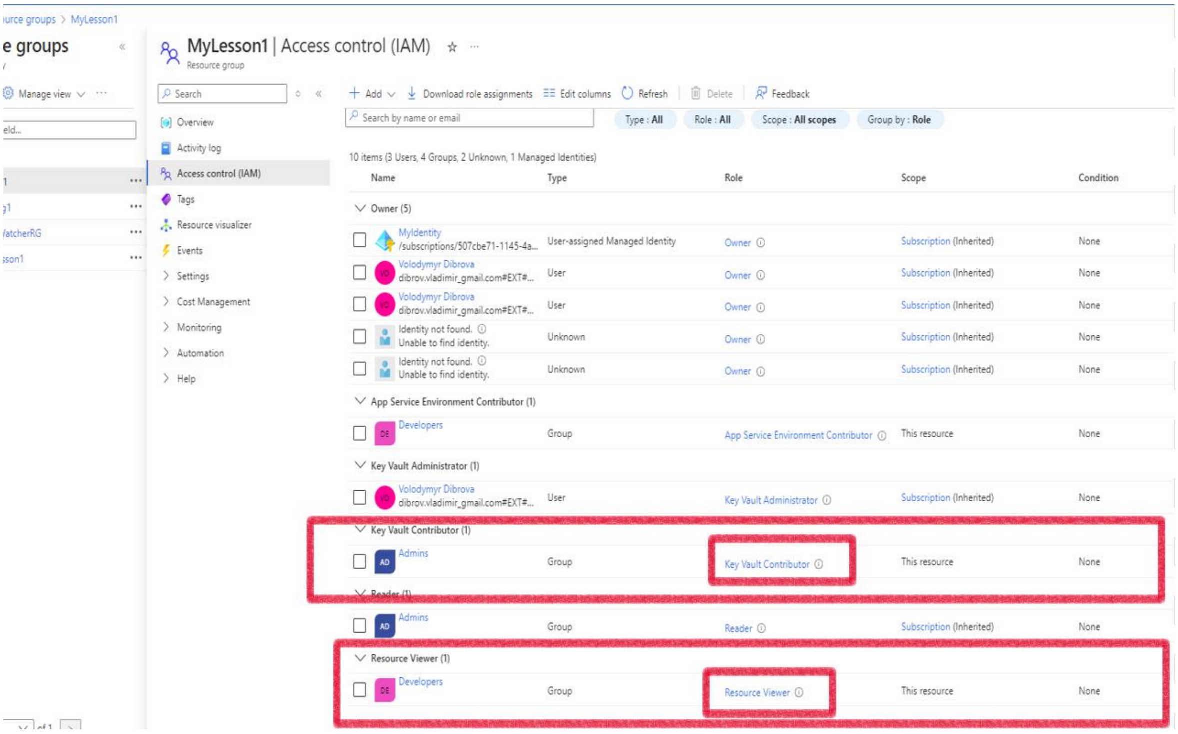
Practical Task 3: Implementing Role-Based Access Control (RBAC)
Implement Role-Based Access Control (RBAC) in Azure to manage access to resources based on roles and
ensure fine-grained access management.

Requirements:

1. Create a custom role named **Resource Viewer** with read-only permissions for a specific resource
group.
2. Assign the **Resource Viewer** role to the **Developers** group created earlier.
3. Assign the built-in **Contributor** role to the **Admins** group for the same resource group.
4. Verify that members of the **Developers** group have only read access and members of the **Admins**
group have full access to the resource group.

Actions Taken:

1. Created a **custom role Resource Viewer** with read-only permissions for a specific resource group.
2. Assigned the **Resource Viewer** role to the **Developers** group created earlier.
3. Assigned the built-in **Contributor** role to the **Admins** group for the same resource group.



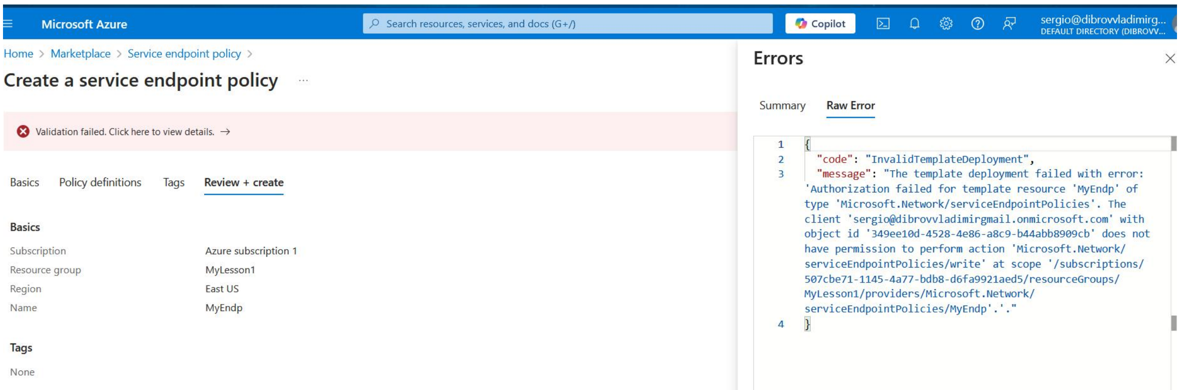
MyLesson1 | Access control (IAM)

Resource group

10 items (3 Users, 4 Groups, 2 Unknown, 1 Managed Identities)

Name	Type	Role	Scope	Condition
Owner (5)				
☐ MyIdentity /subscriptions/507cbe71-1145-4a...	User-assigned Managed Identity	Owner	Subscription (Inherited)	None
☐ Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Owner	Subscription (Inherited)	None
☐ Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Owner	Subscription (Inherited)	None
☐ Identity not found. Unable to find identity.	Unknown	Owner	Subscription (Inherited)	None
☐ Identity not found. Unable to find identity.	Unknown	Owner	Subscription (Inherited)	None
App Service Environment Contributor (1)				
☐ Developers	Group	App Service Environment Contributor	This resource	None
Key Vault Administrator (1)				
☐ Volodymyr Dibrova dibrov.vladimir_gmail.com#EXT#...	User	Key Vault Administrator	Subscription (Inherited)	None
Key Vault Contributor (1)				
☐ Admins	Group	Key Vault Contributor	This resource	None
Reader (1)				
☐ Admins	Group	Reader	Subscription (Inherited)	None
Resource Viewer (1)				
☐ Developers	Group	Resource Viewer	This resource	None

4. Verified access:
    1. Members of the **Developers(Sergio)** group have read-only access.
    2. Members of the **Admins** group have full access to the resource group.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
sergio@dibrovvladimirg...
DEFAULT DIRECTORY (DIBROVV...
Home > Marketplace > Service endpoint policy >
Basics
Policy definitions
Tags
Review + create
Summary
Raw Error

Create a service endpoint policy

Validation failed. Click here to view details. →

Basics

Subscription: Azure subscription 1
Resource group: MyLesson1
Region: East US
Name: MyEndp

Tags

None

Errors

```
{
  "code": "InvalidTemplateDeployment",
  "message": "The template deployment failed with error:
'Authorization failed for template resource 'MyEndp' of
type 'Microsoft.Network/serviceEndpointPolicies'. The
client 'sergio@dibrovvladimirgmail.onmicrosoft.com' with
object id '349ee10d-4528-4e86-a8c9-b44abb8909cb' does not
have permission to perform action 'Microsoft.Network/
serviceEndpointPolicies/write' at scope '/subscriptions/
507cbe71-1145-4a77-bdb8-d6fa9921aed5/resourceGroups/
MyLesson1/providers/Microsoft.Network/
serviceEndpointPolicies/MyEndp'.'."
}
```

Results:

- Successfully configured **Role-Based Access Control (RBAC)** to manage resource access based on predefined roles.

Practical Task 4: Securing Sensitive Information with Azure Key Vault
Set up Azure Key Vault to securely store and manage sensitive information such as keys, secrets, and certificates.

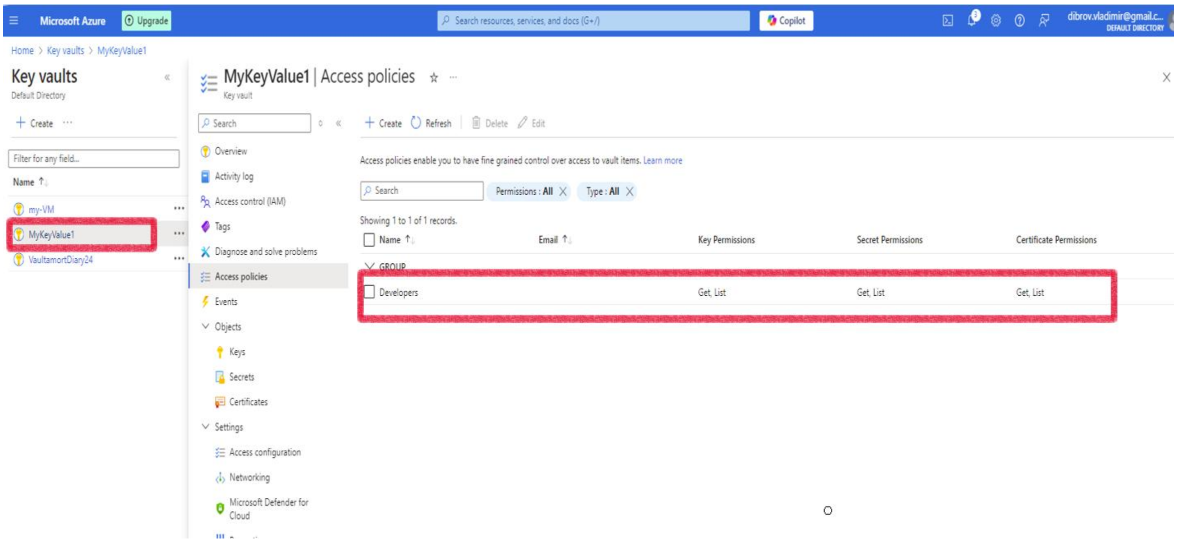
Requirements:

1. Create a new Azure Key Vault in your subscription.
2. Add a secret to the Key Vault (e.g., a database connection string).
3. Set access policies to grant the **Application Developer** role (assigned to the **Developers** group)

permission to retrieve secrets from the Key Vault.
4. Verify that only members of the **Developers** group can access the stored secret.

Actions Taken:

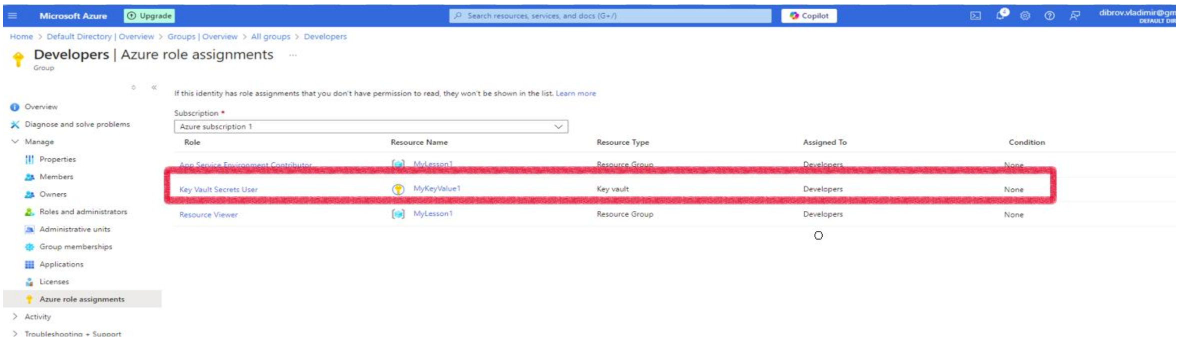
1. Created a new **Azure Key Vault** within the subscription.
2. Added a secret to the Key Vault (database connection string).
3. Configured access policies to grant the **Application Developer** role (assigned to the **Developers** group) permission to retrieve secrets from the Key Vault.



Access policies enable you to have fine grained control over access to vault items. Learn more

Showing 1 to 1 of 1 records.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
GROUP				
Developers		Get, List	Get, List	Get, List

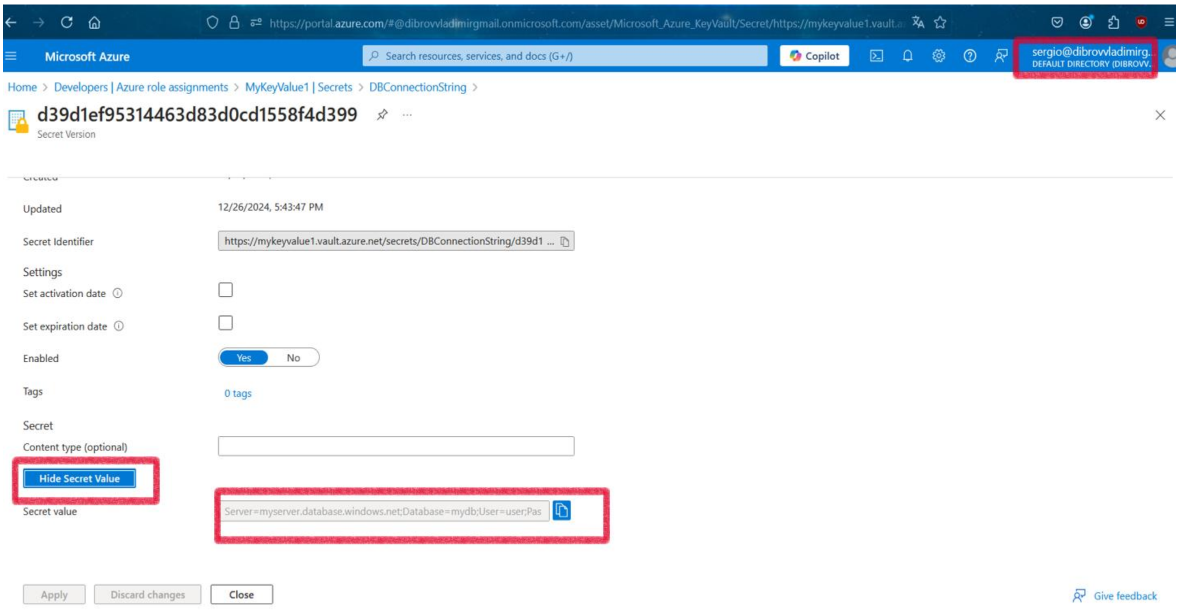


If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *
Azure subscription 1

Role	Resource Name	Resource Type	Assigned To	Condition
App Service Environment Contributor	MyLesson1	Resource Group	Developers	None
Key Vault Secrets User	MyKeyValue1	Key vault	Developers	None
Resource Viewer	MyLesson1	Resource Group	Developers	None

4. Verified access:
    1. Only members of the **Developers** group can access the stored secret.



https://portal.azure.com/#@dibrovvladimirgmail.onmicrosoft.com/asset/Microsoft_Azure_KeyVault/Secret/https://mykeyvalue1.vault.a
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
sergio@dibrovvladimirg.
DEFAULT DIRECTORY (DIBROVV.
Home > Developers | Azure role assignments > MyKeyValue1 | Secrets > DBConnectionString >

d39d1ef95314463d83d0cd1558f4d399

Secret Version

Updated 12/26/2024, 5:43:47 PM

Secret Identifier https://mykeyvalue1.vault.azure.net/secrets/DBConnectionString/d39d1 ...

Settings

Set activation date □

Set expiration date □

Enabled [✓ Yes] No

Tags 0 tags

Secret

Content type (optional)

Secret value Server=myserver.database.windows.net;Database=mydb;User=user;Pas

Apply
Discard changes
Close
Give feedback

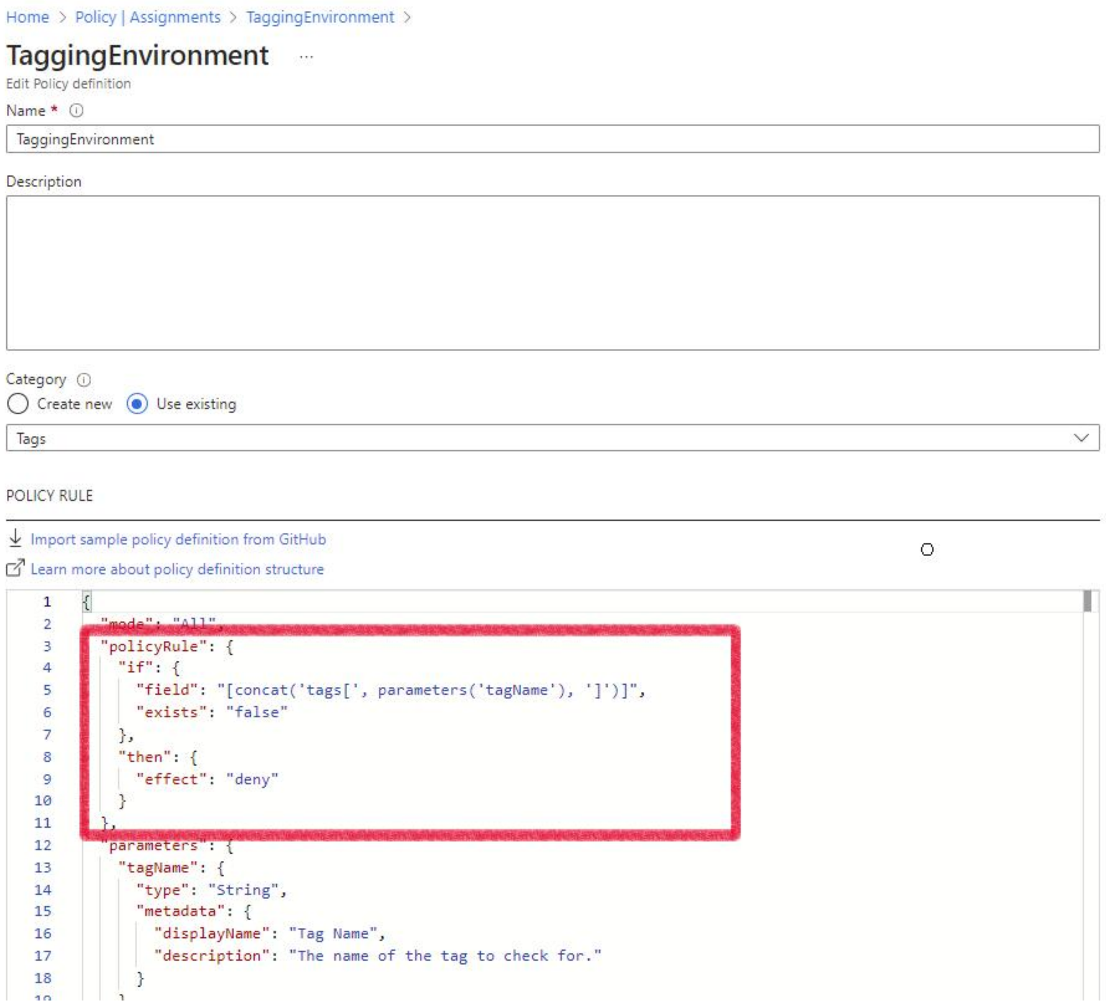
Results:

- Successfully set up **Azure Key Vault** to securely store and manage sensitive information, ensuring restricted access based on roles.

Practical Task 5: Creating and Assigning Basic Azure Policies
Define and assign Azure Policies to enforce compliance with organizational standards for resource
management.
Requirements:
1. Create an Azure Policy to enforce tagging for all newly created resources with a specific tag.
2. Assign the policy to a resource group.
3. Verify that any new resource created in the resource group without the required tag is marked as
non-compliant.
4. Review and document the compliance status of the resource group

Actions Taken:

1. Created an **Azure Policy** to enforce tagging for all newly created resources with a specific tag **Environment: Development**.
2. Assigned the policy to a resource group.



Home > Policy | Assignments > TaggingEnvironment >

TaggingEnvironment ...

Edit Policy definition

Name * ⓘ

TaggingEnvironment

Description

Category ⓘ

○ Create new ● Use existing

Tags

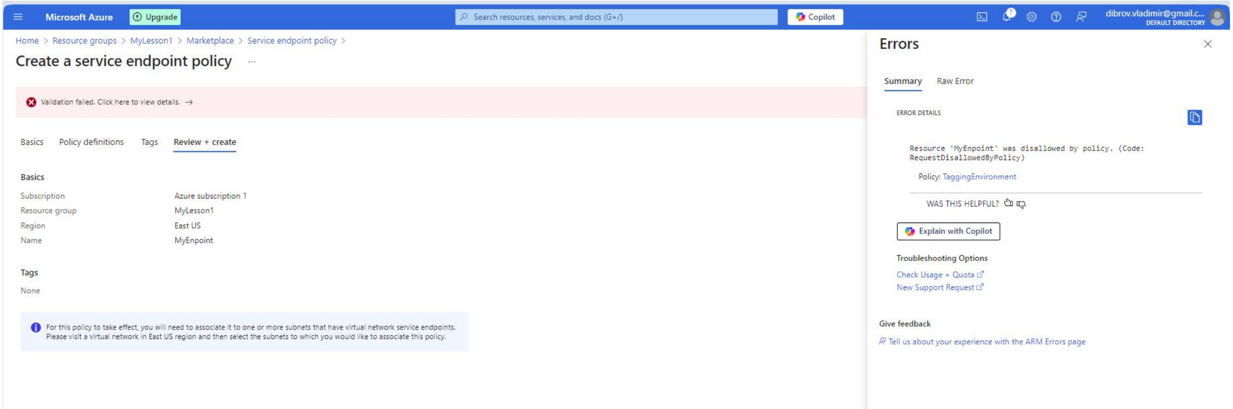
POLICY RULE

Import sample policy definition from GitHub

Learn more about policy definition structure

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "field": "[concat('tags[', parameters('tagName'), ']')]",
      "exists": "false"
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {
    "tagName": {
      "type": "String",
      "metadata": {
        "displayName": "Tag Name",
        "description": "The name of the tag to check for."
      }
    }
```

3. Verified to create resource without tag “Environment”



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
dibrov.vladimir@gmail.c...
DEFAULT DIRECTORY

Home > Resource groups > MyLesson1 > Marketplace > Service endpoint policy >

Create a service endpoint policy ...

Validation failed. Click here to view details. →

Basics | Policy definitions | Tags | Review + create

Basics

Subscription	Azure subscription 1
Resource group	MyLesson1
Region	East US
Name	MyEnpoint

Tags

None

For this policy to take effect, you will need to associate it to one or more subnets that have virtual network service endpoints. Please visit a virtual network in East US region and then select the subnets to which you would like to associate this policy.

Errors

Summary | Raw Error

ERROR DETAILS

```
Resource 'MyEnpoint' was disallowed by policy. (Code:
RequestDisallowedByPolicy)
```

Policy: TaggingEnvironment

WAS THIS HELPFUL?

Explain with Copilot

Troubleshooting Options

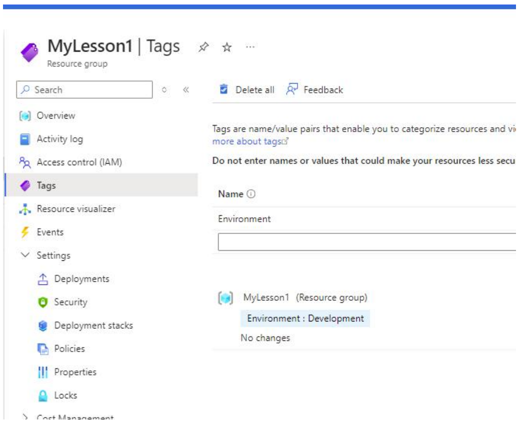
Check Usage + Quota

New Support Request

Give feedback

Tell us about your experience with the ARM Errors page

4. Verified to create resource with tag “Environment”



Tags are name/value pairs that enable you to categorize resources and vi
more about tags

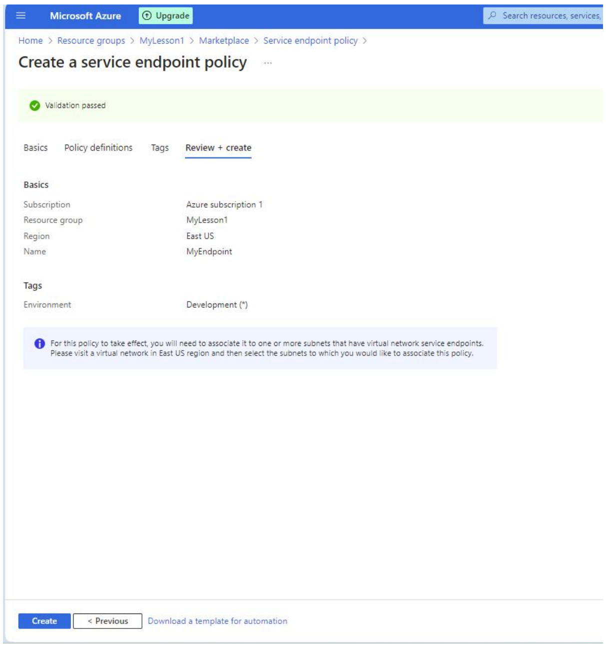
Do not enter names or values that could make your resources less secu

Name: Environment

MyLesson1 (Resource group)

Environment : Development

No changes


Microsoft Azure
Upgrade
Search resources, services,
Home > Resource groups > MyLesson1 > Marketplace > Service endpoint policy >
Basics
Policy definitions
Tags
Review + create
Create
< Previous
Download a template for automation

Create a service endpoint policy

Validation passed

Basics

Subscription	Azure subscription 1
Resource group	MyLesson1
Region	East US
Name	MyEndpoint

Tags

Environment	Development (*)

For this policy to take effect, you will need to associate it to one or more subnets that have virtual network service endpoints. Please visit a virtual network in East US region and then select the subnets to which you would like to associate this policy.

Results:

- Successfully implemented an **Azure Policy** to ensure compliance with organizational standards for resource management.

Practical Task 6: Using Policy Effects to Enforce Compliance

Configure Azure Policies with different policy effects to enforce compliance and manage resources according to organizational standards.

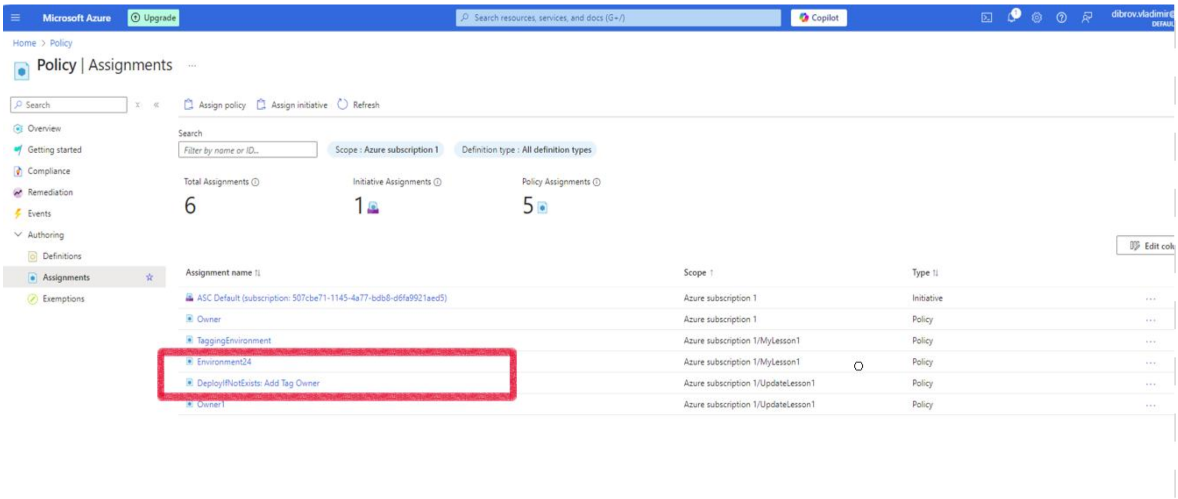
Requirements:

1. Create a policy with the **Audit** effect to monitor and log untagged resources within a resource group.
2. Create a policy with the **DeployIfNotExists** effect to automatically add a specific tag (Owner: IT) to any newly created resource.
3. Assign these policies to a resource group and verify their behavior by:

o Creating a resource without a tag and checking the compliance logs.
o Creating a resource to validate the automatic tag deployment.

Actions Taken:

1. Created a policy with the **Audit** effect to monitor and log untagged resources within a resource group.
2. Created a policy with the **DeployIfNotExists** effect to automatically add a specific tag (**Owner: IT**) to any newly created resource.

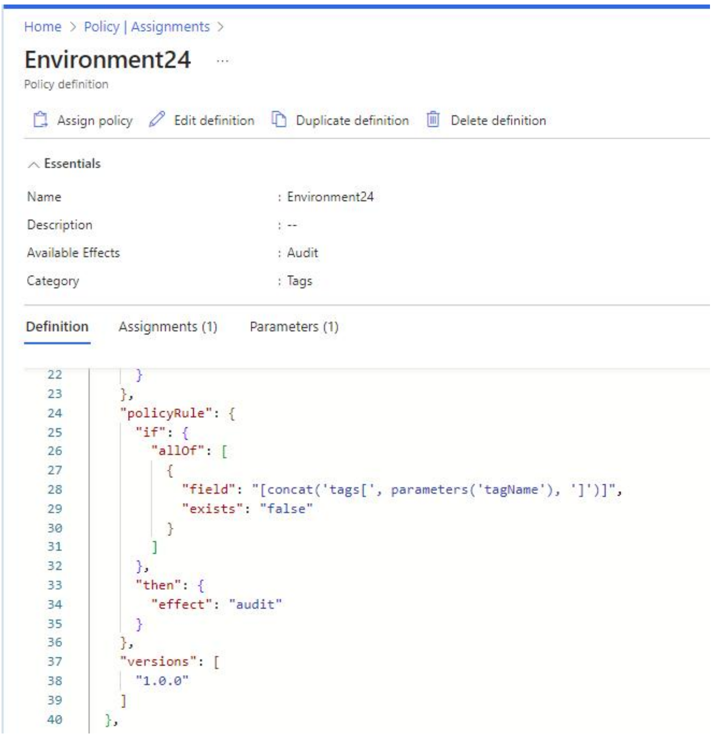


Policy | Assignments

Search: Filter by name or ID...
Scope : Azure subscription 1
Definition type : All definition types

Total Assignments: 6
Initiative Assignments: 1
Policy Assignments: 5

Assignment name	Scope	Type
ASC Default (subscription: 507cbe71-1145-4a77-bdb8-d6fa9921aed5)	Azure subscription 1	Initiative
Owner	Azure subscription 1	Policy
TaggingEnvironment	Azure subscription 1/MyLesson1	Policy
Environment24	Azure subscription 1/MyLesson1	Policy
DeployIfNotExists: Add Tag Owner	Azure subscription 1/UpdateLesson1	Policy
Owner1	Azure subscription 1/UpdateLesson1	Policy

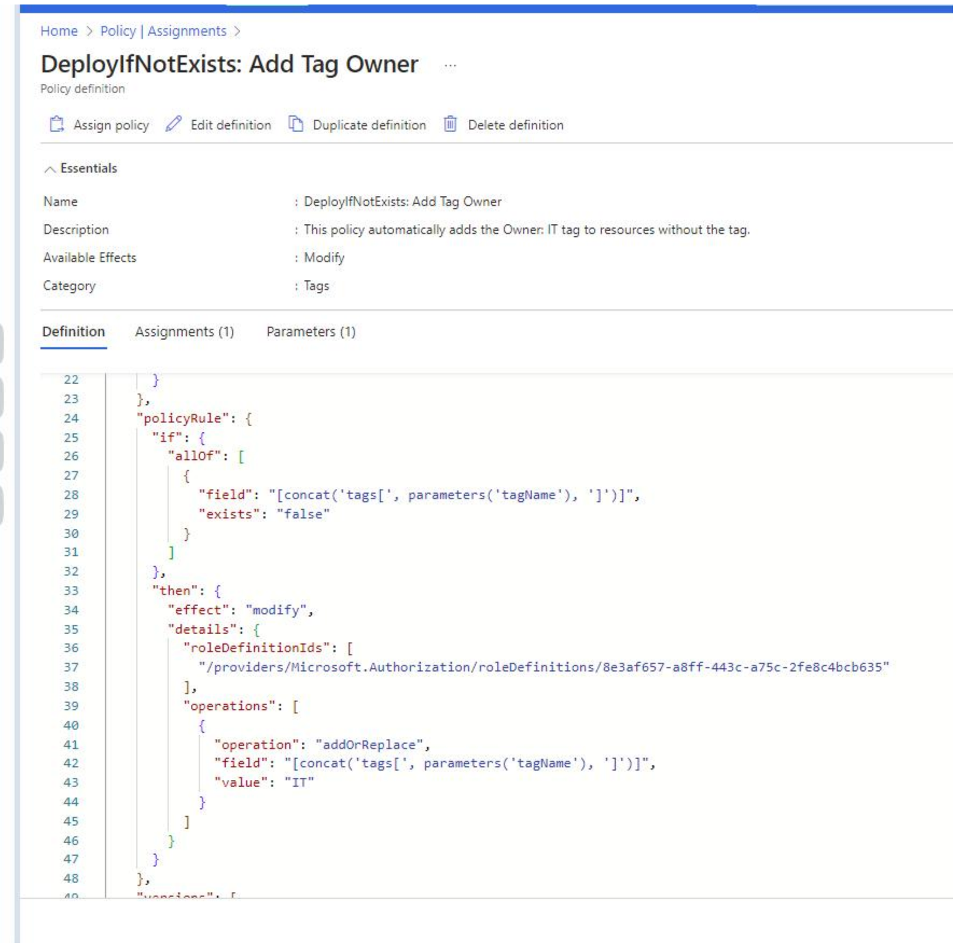


Environment24

Policy definition

Name : Environment24
Description : --
Available Effects : Audit
Category : Tags

```
    }
  },
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "[concat('tags[', parameters('tagName'), ']')]",
          "exists": "false"
        }
      ]
    },
    "then": {
      "effect": "audit"
    }
  },
  "versions": [
    "1.0.0"
  ]
},
```



Home > Policy | Assignments >

DeployIfNotExists: Add Tag Owner ...

Policy definition

Essentials

Name : DeployIfNotExists: Add Tag Owner

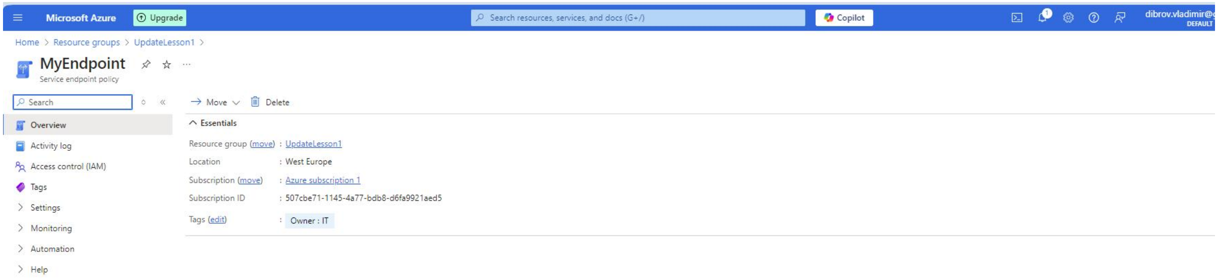
Description : This policy automatically adds the Owner: IT tag to resources without the tag.

Available Effects : Modify

Category : Tags

```
    }
  },
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "[concat('tags[', parameters('tagName'), ']')]",
          "exists": "false"
        }
      ]
    },
    "then": {
      "effect": "modify",
      "details": {
        "roleDefinitionIds": [
          "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635"
        ],
        "operations": [
          {
            "operation": "addOrReplace",
            "field": "[concat('tags[', parameters('tagName'), ']')]",
            "value": "IT"
          }
        ]
      }
    }
  },
  "versions": [
```

3. Assigned both policies to a resource group and verified their behavior:
    1. Created a resource without a tag and checked the compliance logs for auditing.
    2. Created a resource to confirm the automatic deployment of the specified tag.



Home > Resource groups > UpdateLesson1 >

MyEndpoint

Service endpoint policy

Essentials

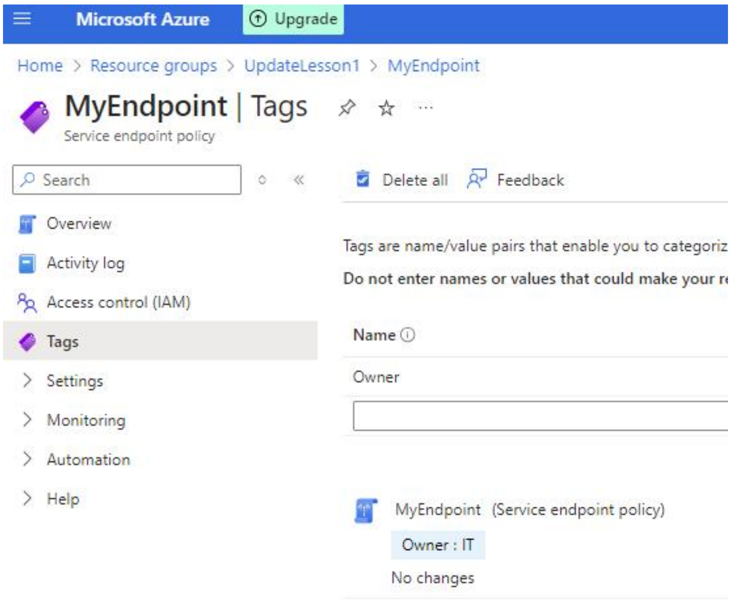
Resource group (move) : UpdateLesson1

Location : West Europe

Subscription (move) : Azure subscription 1

Subscription ID : 507cbe71-1145-4a77-bdb8-d6fa9921aed5

Tags (edit) : Owner : IT



Tags are name/value pairs that enable you to categoriz

Do not enter names or values that could make your r

Name

Owner

MyEndpoint (Service endpoint policy)

Owner : IT

No changes

Results:

- Successfully configured and tested **Azure Policies** with different effects.